CITY RIDGETOP, TENNESSEE
RESOLUTION 23-08

A RESOLUTION TO ADOPT THE CYBER SECURITY PLAN FOR THE CITY OF RIDGETOP, TENNESSEE

WHEREAS, the Tennessee General Assembly adopted PC1111 which requires utilities to prepare and implement a cyber security plan by July 1, 2023 to protect the utility's facilities from unauthorized use, alteration, ransom, or destruction of electronic data and be updated every two years;

WHEREAS, the Board of Mayor and Aldermen, in compliance with guidance from the Comptroller of the Treasury, has created a new cyber security plan, also referenced as a written information security policy (WISP);

NOW, THEREFORE, BE IT RESOLVED by the Board of Mayor and Aldermen of the City of Ridgetop, Tennessee that the following is hereby approved:

Section 1. The City of Ridgetop adopts the Cyber Security Plan named *Written Information Security Plan* dated June 2023 in Exhibit A.

Section 2. This Resolution takes effect immediately upon its passage, the public welfare requiring it.

Approved this 20 day of June, 2023.

____

Mayor Tim Shaw

Attest: __________________________________

City Recorder

EXHIBIT A.

Statement of Policy

The objective of the City of Ridgetop, Tennessee in the development and implementation of this comprehensive Written Information Security Policy ("WISP"), is to create effective administrative, technical and physical safeguards for the protection of personally identifiable information (PII) of customers, clients and employees as well as sensitive City information that could\harmful if unauthorized access were to occur. The WISP sets forth a procedure for evaluating and addressing electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting PII and sensitive City information.

*The use of the term **employees** will include all of the City's management, employees, all independent contractors and temporary employees.*

Purpose of Policy

The purpose of the WISP is to better:

1) Ensure the security and confidentiality of **personally identifiable information (PII)** of customers, clients, employees or vendors as well as **sensitive city data** which includes emails, confidential city information (i.e., city expansion plans, manufacturing processes, highly secretive information, etc.), employee information and the like.;
2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information; and
3) Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft, fraud or harm to the city.

Scope of Policy

In formulating and implementing the WISP, The City has addressed and incorporated the following protocols:

1) Identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PII and sensitive City data.
2) Assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the PII and sensitive City data.
3) Evaluated the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risk.
4) Designed and implemented a WISP that puts safeguards in place to minimize identified risks.
5) Implemented regular monitoring of the effectiveness of those safeguards.

Security Safeguards

The follow safeguards are effective immediately. The goal of implementing these safeguards is to protect against risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PII or sensitive City data.

Administrative Safeguards

1) **Security Officer -** The City has designated the **City Recorder** to implement, supervise and maintain the WISP. This designated employee (the "Security Officer") will be responsible for the following:
   a) Implementation of the WISP including all provisions outlined in **Security Safeguards.**
   b) Training of all employees that may have access to PII and sensitive City data. Employees should receive annual training and new employees should be trained as part of the new employee hire process.
   c) Regular monitoring of the WISP's safeguards and ensuring that employees are complying with the appropriate safeguards.
   d) Evaluating the ability of any third-party service providers to implement and maintain appropriate security measures for the PII and sensitive City data to which the city has permitted access, and requiring third-party service providers, by contract, to implement and maintain appropriate security measures.
   e) Reviewing all security measures at least annually, or whenever there is a material change in the city's business practices that may put PII and sensitive city data at risk.
   f) Investigating, reviewing and responding to all security incidents or suspected security incidents.

2) **Security Management-** All security measures will be reviewed at least annually, or whenever there is a material change in the city's business practices that may put PII or sensitive city data at risk. This should include performing a security risk assessment, documenting the results and implementing the recommendations of the security risk assessment to better protect PII and sensitive city data. The Security Officer will be responsible for this review and will communicate to management the results of that review and any recommendations for improved security arising out of that review.

3) **Minimal Data Collection-** The City will only collect PII of clients, customers or

   employees that is necessary to accomplish legitimate business transactions or to comply with any and all federal, state or local regulations.

4) **Information Access-** Access to records containing PII and/or sensitive city data shall be limited to those persons whose job functions requires a legitimate need to access the records. Access to the records will only be for a legitimate job-related purpose. In addition, pre-employment screening should take place to protect PII and sensitive city data.

5) **Employee Termination-** Terminated employees must return all records containing PII and sensitive city data, in any form, that may be in the former employee's possession (including all information stored on laptops or other portable devices or media, and in files, records, work papers, etc.). A terminated employee's physical and electronic access to PII and sensitive city data must be immediately blocked. A terminated employee shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to the city's premises or information. A terminated employee's remote electronic access to PII and sensitive city data must be disabled; his/her voicemail access, e-mail access, internet access, and passwords must be invalidated.

6) **Security Training-** All employees, which includes all owners, managers, employees, all independent contractors and temporary employees that may have access to PII and sensitive city data, will receive security training. Employees should receive at least annual training and new employees should be trained as part of the new employee hire process. Employees should be required to show their knowledge of the information and be required to pass an exam that demonstrates their knowledge. Documentation of employee training should be kept and reviewed.

7) **WISP Distribution-** A copy of the WISP is to be distributed to each current employee and to each new employee on the beginning date of their employment. It shall be the employee's responsibility for acknowledging in writing or electronically, that he/she has received a copy of the WISP and will abide by its provisions.

8) **Contingency Planning-** All systems that store PII and/or sensitive city data should have the data backed up on, at least, a nightly basis. Data should be encrypted and be stored offsite. Disaster Recovery mechanisms and documented procedures should be in place to restore access to PII and sensitive city data as well as any operational systems that the city relies on. A system criticality assessment should be performed that defines how critical each of The City's systems are. Systems that are critical to operations should be restored before non-critical systems. On a periodic basic, data backups, data restoration and Disaster Recovery procedures should be tested and validated.

9) **Security Incident Procedures-** Employees are required to report suspicious or unauthorized use of PII and/or sensitive city data to a supervisor or the Security Officer. Whenever there is an incident that requires notification pursuant to any federal or state regulations, the Security Officer will conduct a mandatory post-incident review of the events and actions taken in order to determine how to alter security practices to better safeguard PII and sensitive data.

10) **Emergency Operations-** Procedures should be in place to define how the city will respond to emergencies. Procedures should include employee contact information, critical vendor contact information, important vendor account information as well as any emergency operating procedures.

11) **Data Sensitivity Classification-** All data that the city stores or accesses should be categorized in terms of the sensitive nature of the information. For example, PII and sensitive city data might have a very high sensitivity and should be highly protected whereas publicly accessible information might have a low sensitivity and requires minimal protection.

12) **Third-Party Service Providers-** Any service provider or individual ("Third-Party Service Provider") that receives, stores, maintains, processes, or otherwise is permitted access to any file containing PII and/or sensitive city data shall be required to protect PII and sensitive city data. The Third-Party Service Providers must sign service agreements that contractually hold them responsible for protecting the city's data. Examples include third-parties who provide off-site backup of electronic data, website hosting companies, credit card processing companies, paper record copying or storage providers, IT/ Technology Support vendors, contractors or vendors working with customers and having authorized access to PII and/or sensitive city data.

13) **Sanctions-** All employment contracts, where applicable, should be amended to require all employees to comply with the provisions of the WISP and to prohibit any nonconforming use of PII and/or sensitive city data as defined by the WISP. Disciplinary actions will be taken for violations of security provisions of the WISP. The nature of the disciplinary measures may depend on a number of factors including the nature of the violation and the nature of the PII and/or sensitive City data affected by the violation.

14) **Bring Your Own Device (BYOD) Policy-** The City may allow employees to utilize personally owned devices such as laptops, smartphones and tablets. If allowed, proper safeguards must be implemented to protect PII and sensitive City data that may be accessed or stored on these devices. Employees must understand what are the requirements for using personally owned devices and what safeguards are required.

Physical Safeguards

15) **Facility Access Controls-** The City will implement physical safeguards to protect PII and sensitive City data. There will be physical security on buildings to prevent unauthorized access. All systems that access or store PII and/or sensitive City data will be physically locked. Employees **will** be required to maintain a "clean desk" and ensure that PII and/or sensitive City data is properly secured when they are not at their desk. The Security Officer will maintain a list of lock combinations, passcodes, keys,etc. and which employees that have access to the facilities and PII and/or sensitive data. Visitors will be restricted from areas that contain PII and/or sensitive city data.

16) **Network Security-** The City will implement security safeguards to protect PII and sensitive city data. Safeguards include isolating systems that access or store PII and/or sensitive City data, the use of encryption on all portable devices, physical protection on portable devices, ensuring that all systems run up-to-date anti-malware, implementing network firewalls, performing periodic vulnerability scans, capturing and retaining network log files as well as ensuring that servers and critical network equipment are stored in an environmentally safe location.

Technical Safeguards

17) **Access Control -** Access to PII and sensitive city data shall be restricted to approved active users and active user accounts only. Employees will be assigned unique user accounts and passwords. Systems containing PII and sensitive city data should have automatic logoff procedures to prevent unauthorized access.

18) **Computer Use -** All employees will be given a Computer Use Policy that defines acceptable and unacceptable use of the city's computing resources. Employees should be required to sign the Computer Use Policy to acknowledge acceptance of the policy.

19) **Data Disposal** -Written and electronic records containing PII and sensitive city data shall be securely destroyed or deleted at the earliest opportunity consistent with business needs or legal retention requirements.

20) **System Activity Review-** All systems that store or access PII and sensitive City data should utilize a mechanism to log and store system activity. Periodic system activity reviews should occur and identify unauthorized access to PII and sensitive city data. Any unauthorized access should be reported to the Data Security Coordinator.

21) **Encryption-** To the extent technically feasible all portable devices that contain PII and sensitive City data should be encrypted to protect the contents. In addition, encryption should be used when sending any PII and sensitive city data across public networks and wireless networks. Public networks include email and Internet access.

Cybersecurity Response Plan

Being prepared to respond to a cyber-attack will reduce the impact that it has on office operations. It is imperative that the City of Ridgetop have a written plan that can be referenced in the event the office experiences an incident. The following plan has been developed in cooperation with the City of Ridgetop and third-part vendor Tyler Technologies.

This document is being provided for the purpose of assisting our customers with responding to questions regarding cybersecurity that may asked during an audit. However, it is not intended to provide a detailed analysis and review of all components that make up a system. Due to the wide variety of computers, operating systems, network components, and peripherals of varying age that exist at _____customer offices, the answers provided below primarily address systems that were purchased directly from Tyler Technologies and are not obsolete due to age or OEM retirement. Systems that are obsolete or purchased/maintained by a provider other than Tyler Technologies are not addressed in the responses below. Additionally, these responses are general in nature, therefore, variances at individual customer offices are likely.

Tyler Technologies offers a wide range of Cybersecurity services to better secure customer data including antivirus software, a cloud-based and local backup solution, advanced monitoring, and detection software, as well as multi-factor authentication. Detailed information regarding these services is listed below including how they help protect against cyberattacks and Tyler Technologies response should a breach occur. The City of Ridgetop has a contract with Tyler Technologies to provide the following protections.

Antivirus

Protection

Tyler Technologies cloud-based, business class antivirus software helps detect, prevent, scan, and delete malware (malicious software) and viruses. The software runs automatically in the background to provide protection against

Response

Once contacted by the customer regarding the concern of an infection, Tyler Technologies will investigate. If Tyler Technologies determines there is an infection, then the computer would be cleaned of the virus or virus attacks. It is comprehensive virus protection to help protect files and hardware from malware such as worms, Trojan horses, and spyware. Tyler Technologies antivirus software includes an auto-clean feature that deletes harmful software, automatic update for new types of malwares, protection against multiple types of malwares across multiple applications, and scanning for the presence of malware.

reloaded if necessary.

Contact Phone: 800-646-2633

Backups (Local & Cloud)

Protection

Tyler Technologies One Backup combines local and online backups into a single product. All the details of the backups are available in an easy-to-read interface, including when an individual file was last backed up or the status of the backups. Restoring a file or folder is just as simple as locating a file in Windows. Tyler Technologies monitors the backups to confirm the Cloud as well as local media (SSD Drives/Thumb Drives) backups were successful.

Response

Multiple versions of the customers' files are backed up daily. In the event the most recent version of the backup is encrypted or corrupted, Tyler Technologies can easily restore an earlier version. Cloud backup storage cannot be modified from the user side, so backups cannot be removed.

Tyler Technologies Cybersecurity Information

How are operating system updates applied to workstations and servers? Are these updates installed automatically or on a set schedule so that all current updates are installed timely?

During installation, all computer software purchased from Tyler Technologies are set to automatically update daily and apply updates regularly.

Additionally, Tyler Technologies offers an optional managed network service to monitor the customer's Tyler Technologies servers to ensure all critical updates are verified and applied in a timely manner.

Are software and database patches applied to accounting software?

SQL updates are applied through windows updates.

Software updates are automatically applied to Tyler Technologies cloud hosted software. Software updates are made available to customers for download for all other Tyler Technologies on premise software.

Do the workstations and servers have antivirus software installed? Is this software configured to receive definition updates automatically? How often does it run a scan to detect malicious software?

Tyler Technologies recommends antivirus software for all computers purchased. If the customer chooses to purchase antivirus software, it is configured to scan periodically for threats and automatically apply any manufacturer updates as they become available. VC3 manages the Malwarebytes software that scans for malicious malware.

Do you allow remote access to your system via VPN, remote desktop software, or other means? What product is used and how is it secured?

Tyler Technologies will configure remote access only upon request by the customer. Tyler Technologies offers both VPN and remote connection software. Each have 256-bit encryption plus password complexity to help secure the connections.

Do you ever perform vulnerability scans of the network?

Upon request, VC3 may perform a vulnerability scan when asked for a specific reason.

Does the backup process capture all data vital to the operation of the office? In addition to the accounting system, are other critical files such as spreadsheets and documents backed up?

At time of installation, Tyler Technologies configures the backup to capture all critical data pertaining to the Tyler Technologies software along with any data on the C drive and other folders specified by the customer.

If the office were to fall victim to a ransomware attack, is the backup process configured so that backup data would not

Tyler Technologies performs a daily backup of media for each day of the week Monday-Friday.

be encrypted in the attack?

Are there any other measures in place to protect the office from a cyberattack?

Several times throughout the year Tyler Technologies communicates with our customers the importance of backups, offsite and cloud backups, antivirus and malware software and the importance of keeping all hardware current and updated.

Procedures:

1. What should we do if we receive a ransom request, or accidentally click on an email that has a virus? (Should we turn the computer off?)

Answer: Viruses can take many different shapes. Your first line of defense is the firewall which inspects incoming packets and your email server's antivirus checking messages. Assuming one gets through those, your next line is endpoint security or your workstation antivirus. All of the workstations at City Hall have Bitdefender installed which provides another layer of protection. If Bitdefender is tripped, it may be able to remove or quarantine the offending file or block an offending website and just notify you. If it cannot remove it, it will attempt to delete it. If unable to do either, you would want to isolate the computer from the network by either shutting it down or unplugging the network cable. Feel free to contact us at any point along the way. We'll help you through it.

If you have a case of ransomware or malware, you would want to power it off or unplug the network cable as quickly as possible to keep it from moving to other devices via share folders, such as to the server or other workstations. The workstation/server would need to be scanned, cleaned, and in severe cases, reloaded before being put back on the network. I

2. Do we have an inventory of each computer and what kind of data is stored on each?

Answer: I am not aware of the City actively tracking computer/server inventories nor the data store on them. Tyler Technologies does not maintain any such database. It is beyond the scope of Network Support. Hardware purchased from Tyler Technologies is recorded in our customer system for devices on active hardware maintenance support.

3. What kind of operational plan would we need to adopt if the system had to be restored?

Answer: Not quite sure this is what you are wanting but generally speaking, should a computer need restored, if it is not "cleaned" or is "not trusted" after an event, any backups should be made of the data on the system or, if previously performed, verified as available, the computer should remain off the network until the hard drive is reformatted and the operating system re-installed. The computer can then be placed back on the network and data restored, if available.

Cyber Security Insurance:	**Public Entity Partners** **615- 371-0049** **Policy Number: ??????????????**

Incident Response Procedure

Contents

Step	Incident Response Procedure	Action	Date Completed

Detection & Analysis

1. Declare Incident

1a.	Perform initial categorization of incident.		
1b.	Designate organizational incident coordination lead.		
1c.	In accordance with preparation policies and plans, provide internal notification to organizational leadership, system owner, and marketing department; if applicable, law enforcement.		

2. Determine Investigation Scope

2a.	Identify the type and extent of the incident.		
2b.	Assess operational or informational impact on organization's mission.		

3. Collect and Preserve Data

3a.	Collect and preserve the data necessary for incident verification, categorization, prioritization, mitigation, reporting, attribution, and as potential evidence in accordance with NIST 800-61r2.		
3b.	Log all evidence and note how the evidence was acquired, when it was acquired, and who acquired the evidence.		

4. Perform Technical Analysis

4a.	Develop a technical and contextual understanding of the incident.		
4b.	Based on analysis thus far and available CTI, form a hypothesis of what the adversary was attempting to access/accomplish.		
4c.	Update scope as investigation progresses and information evolves. Report most recent findings and incident status to parties outlined in 1c.		
4d.	**Terminating condition:** Technical analysis is complete when the incident has been verified, the scope has been determined, the method(s) of persistent access to the network has/have been identified, the impact has been assessed, a hypothesis for the narrative of exploitation has been cultivated (TTPs and IOCs), and all stakeholders are proceeding with a common operating picture.		

Step	Incident Response Procedure	Action Taken	Date Completed
Correlate Events and Document Timeline			
4e.	Analyze logs to correlate events and adversary activity		
4f.	Establish an incident timeline that records events, description of events, date-time group (UTC) of occurrences, impacts, and data sources. Keep updated with all relevant findings.		
Identify Anomalous Activity			
4g.	Assess affected systems and networks for subtleties of adversary behavior which often may look legitimate.		
4h.	Identify deviations from established baseline activity - particularly important to identify attempts to leverage legitimate credentials and native capabilities and tools (i.e., living off the land techniques).		
Identify Root Cause and Enabling Conditions			
4i.	Attempt to identify the root cause of the incident and collect threat information that can be used in further searches and inform subsequent response efforts.		
4j.	Identify and document the conditions that enabled the adversary to access and operate within the environment.		
4k.	Assess networks and systems for changes that may have been made to either evade defenses or facilitate persistent access.		
4l.	Identify attack vector. This includes how the adversary accessing the environment (e.g., malware, RDP, VPN).		
4m.	Assess access (depth and breadth). This includes All compromised systems, users, services, and networks.		
Gather Incident Indicators			
4n.	Review available CTI for precedent of similar activity.		
4o.	Analyze adversary tools. Assess tools to extract IOCs for short-term containment.		
4p.	Identify and document indicators that can be used for correlative analysis on the network.		
4q.	Share extracted threat information (atomic, computed, and behavioral indicators, context, and countermeasures) with internal response teams and pertinent parties.		

Step	Incident Response Procedure	Action Taken	Date Completed
Analyze for Common Adversary TTPs			
4r.	Identify initial access [TA0001] techniques (e.g., spear phishing, supply chain compromise).		
4s.	If access is facilitated by malware, identify associated command and control [TA0011] (e.g., identify port, protocol, profile, domain, IP address).		
4t.	Identify the techniques used by the adversary to achieve code execution [TA0002].		
4u.	Assess compromised hosts to identify persistence [TA0003] mechanisms.		
4v.	Identify lateral movement [TA0008] techniques. Determine the techniques used by the adversary to access remote hosts.		
4w.	Identify the adversary's level of credential access [TA0006] and/or privilege escalation.		
4x.	Identify the method of remote access, credentials used to authenticate, and level of privilege. If access is by legitimate but compromised application (e.g., RDP. VPN), identifies the method.		
4y.	Identify mechanism used for data exfiltration [TA0010].		
Validate and Refine Investigation Scope			
4z.	Identify new potentially impacted systems, devices, and associated accounts.		
4aa.	Feed new IOCs and TTPs into detection tools.		
4bb.	Continue to update the scope and communicate updated scope to all stakeholders to ensure a common operating picture.		
5. Third-Party Analysis Support (if needed)			
5a.	Identify if third-party analysis support is needed for incident investigation or response.		
5c.	Coordinate and facilitate access if incorporating third-party analysis support into response efforts.		

Step	Incident Response Procedure	Action Taken	Date Completed
6. Adjust Tools			
6a.	Tune tools to slow the pace of advance and decrease dwell time by incorporating IOCs to protect/detect specific activity.		
6b.	Introduce higher-fidelity modifications to tools. Tune tools to focus on tactics that must be used by the adversary to obtain operational objectives (e.g., execution, credential access, and lateral movement).		
Containment			
7. Contain Activity (Short-term Mitigations)			
7a.	Determine appropriate containment strategy, including: • Requirement to preserve evidence • Availability of services (e.g., network connectivity, services continuity) • Resource constraints • Duration of containment steps		
7b.	System backup(s) to preserve evidence and continued investigation.		
7c.	Coordinate with law enforcement to collect and preserve evidence (as required by (Step 3a) prior to eradication, if applicable.		
7d.	Isolate affected systems and networks including: • Perimeter containment • Internal network containment • Host-based/Endpoint containment • Temporarily disconnect public-facing systems from the Internet, etc.		
7e.	Close specific ports and mail servers. Update firewall filtering.		
7f.	Change system admin passwords, rotate private keys and service/application account secrets where compromise is suspected revoke privileged access.		
7g.	Perform blocking (and logging) of unauthorized accesses, malware sources, and egress traffic to known attacker Internet Protocol (IP) addresses.		
7h.	Prevent Domain Name Server (DNS) resolution of known attacker domain names.		
7i.	Prevent compromised system(s) from connecting to other systems on the network.		
7j.	Direct adversary to sandbox to monitor activity, gather additional evidence, and identify TTPs.		
7k.	Monitor for signs of threat actor response to containment activities.		
7l.	Report updated timeline and findings (including new atomic and behavioral indicators) to pertinent parties.		

Step	Incident Response Procedure	Action Taken	Date Completed
7m.	If new signs of compromise are found, return to technical analysis (Step 4) to re-scope the incident.		
7n.	**Terminating condition:** Upon successful containment (i.e., no new signs of compromise), preserve evidence for reference and law enforcement investigation (if applicable), adjust detection tools, and move to eradication.		

Eradication & Recovery

8. Execute Eradication Plan

8a.	Develop a well-coordinated eradication plan that considers scenarios for threat actor use of alternative attack vectors and multiple persistence mechanisms.		
8b.	Provide incident status until all eradication activities are complete.		
8c.	Remove artifacts of the incident from affected systems, networks, etc.		
8d.	Reimage affected systems from clean backups (i.e., 'gold' sources).		
8e.	Rebuild hardware (if rootkits involved).		
8f.	Scan for malware to ensure removal of malicious code.		
8g.	Monitor closely for signs of threat actor response to eradication activities.		
8h.	Allow adequate time to ensure all systems are clear of threat actor persistence mechanisms (such as backdoors) since adversaries often use more than one mechanism.		
8i.	Update the timeline to incorporate all pertinent events from this step.		
8j.	Complete all actions for eradication.		
8k.	Continue with detection and analysis activities after executing the eradication plan to monitor for any signs of adversary re-entry or use of new access methods.		
8l.	If new adversary activity is discovered at the completion of the eradication step, contain the new activity and return to Technical Analysis (Step 4) until the true scope of the compromise and infection vectors are identified.		
8m.	If eradication is successful, move to Recovery.		

9. Restore

9a.	Restore agency systems to operational use: recovering mission/business data.		

Step	Incident Response Procedure	Action Taken	Date Completed
9b.	Revert all changes made during incident.		
9c.	Reset passwords on compromised accounts.		
9d.	Implement multi-factor authentication for all access methods.		
9e.	Install updates and patches.		
9f.	Tighten perimeter security (e.g., firewall rulesets, boundary router access control lists) and zero trust access rules.		
9g.	Test systems thoroughly (including security controls assessment) to validate systems are operating normally before bringing back online in production networks.		
9h.	Consider emulating adversarial TTPs to verify countermeasures are effective.		
9i.	Review all relevant CTI to ensure situational awareness of the threat actor activity.		
9j.	Update incident timeline to incorporate all pertinent events from Recovery step.		
9k.	Complete all actions for recovery.		

Post-Incident Activities

10. Post-Incident Activities

10a.	Document the incident, inform agency leadership, harden the environment to prevent similar incidents, and apply lessons learned to improve the handling of future incidents.		

Adjust Sensors, Alerts, and Log Collection

10b.	Add enterprise-wide detections to mitigate against adversary TTPs that were successfully executed.		
10c.	Identify and address operational "blind spots" to adequate coverage moving forward.		
10d.	Continue to monitor the agency environment for evidence of persistent presence.		

Step	Incident Response Procedure	Action Taken	Date Completed
Finalize Reports			
10e.	Provide post-incident updates as required by law and policy.		
10f.	Publish post-incident report. Provide a step-by-step review of the entire incident and answer the Who, What, Where, Why, and How questions.		
Perform Hotwash			
10g.	Conduct lessons learned analysis with all involved parties to assess existing security measures and the incident handling process recently experienced.		
10j.	Identify if IR processes were followed and if they were sufficient.		
10k.	Identify any policies and procedures in need of modification to prevent similar incidents from occurring.		
10l.	Identify how information sharing with stakeholders can be improved during IR.		
10m.	Identify any gaps in incident responder training.		
10n.	Identify any unclear or undefined roles, responsibilities, interfaces, and authorities.		
10o.	Identify precursors or indicators that should be monitored to detect similar incidents.		
10p.	Identify if infrastructure for defense was sufficient. If not, identify the gaps.		
10q.	Identify if additional tools or resources are needed to improve detection and analysis and help mitigate future incidents.		
10r.	Identify any deficiencies in the incident response planning process. If no deficiencies identified, identify how the organization intends to implement more rigor in its IR planning.		